Draft Paper

16th ICCRTS

"Collective C2 in Multinational Civil-Military Operations"

Privacy Preserving Service Discovery for Interoperability in Power to the Edge Approach

Topic 1: Concepts, Theory, and Policy

Topic 3: Information and Knowledge Exploration

Topic 9: Networks and Networking

Authors:

Hiroshi Yamaguchi, Masahito Gotaishi, Shigeo Tsujii, Norihisa Doi

Research and Development Initiative, Chuo University

1-13-27, Kasuga Bunkyo-ku, Tokyo 112-8551, Japan

Point of Contact

Hiroshi Yamaguchi

yamaguchivc@cap.ocn.ne.jp

Research and Development Initiative, Chuo University

1-13-27, Kasuga Bunkyo-ku, Tokyo 112-8551, Japan

Tel: +81-3-3817

Additional Point of Contact

Masahito Gotaishi gotaishi@tamacc.chuo-u.ac.jp; mgota@r6.dion.ne.jp

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Privacy Preserving Service Discovery for Interoperability in Power to the Edge Approach	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Chuo University,Research and Development Initiative,1-13-27, Kasuga Bunkyo-ku,Tokyo 112-8551, Japan,**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Presented at the 16th International Command and Control Research and Technology Symposium (ICCRTS 2011), Qu?c City, Qu?c, Canada, June 21-23, 2011. U.S. Government or Federal Rights License.

14. ABSTRACT
As the networks become large-scale, they include various confidential data which need strict access control. Then we face the problem of satisfying the conflicting requirements of confidentiality and utilization. Access should be allowed when the information is necessary in performing the duty, although, in some cases, full access is not necessary when the data is used to compute statistics. Such unnecessary disclosure is required under existing access-control system. A typical case is the medical information system. For example, it should be kept confidential that ?Mr. Smith of age 37 is suffering from hypertension.? In some public health studies, scientists might have to compute ?mean blood pressure of men in their thirties.? In such cases, they do not have to know the blood pressure of Mr. Smith, but in the existing access-control system, it must be disclosed just in order to compute the average. Data processing, such as computing average and correlation, is enabled without disclosing the actual value, by using cryptosystem and cryptographic protocol. We propose a medical network system utilizing the new access-control system and new cryptographic protocol, thereby realizing active data sharing and interoperability between medical network and non-medical networks, such as disaster countermeasures or nursing care network.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**27**	

Abstract

As the networks become large-scale, they include various confidential data which need strict access control. Then we face the problem of satisfying the conflicting requirements of confidentiality and utilization. Access should be allowed when the information is necessary in performing the duty, although, in some cases, full access is not necessary when the data is used to compute statistics. Such unnecessary disclosure is required under existing access-control system.

A typical case is the medical information system. For example, it should be kept confidential that “Mr. Smith of age 37 is suffering from hypertension.” In some public health studies, scientists might have to compute “mean blood pressure of men in their thirties.” In such cases, they do not have to know the blood pressure of Mr. Smith, but in the existing access-control system, it must be disclosed just in order to compute the average. Data processing, such as computing average and correlation, is enabled without disclosing the actual value, by using cryptosystem and cryptographic protocol.

We propose a medical network system utilizing the new access-control system and new cryptographic protocol, thereby realizing active data sharing and interoperability between medical network and non-medical networks, such as disaster countermeasures or nursing care network.

1. Introduction

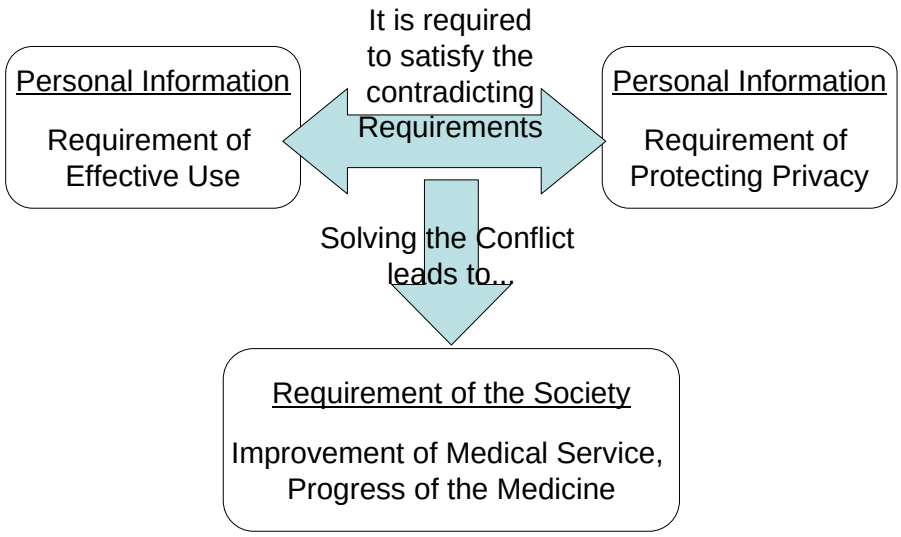
From the aspect of organization theory, the core concept of “Power to the Edge” is the cooperation among different organizations with different cultures and behavior, such as the army and non-government organizations (NGOs). Various effort and training would be required for each participant, besides technology infrastructure, which enables them to share information is necessary. The field for which network-centric operation is proposed is healthcare. Cooperation among medical organizations and nursing care organizations is especially important in the current aging society.

Like Global Information Grids (GIGs) in the “Power to the Edge,” large-scale Information Technology (IT) infrastructures such as the “Worldwide Healthcare Information Grid (WHIG)” have been proposed [1]. The shared situation awareness and interoperability between physicians and service care providers, or physicians and public health experts, would extensively improve the effectiveness of healthcare. Although the benefit of sharing information would be obvious, there are concerns related to information security.

Undoubtedly there is a security requirement that the confidential information, such as the name of the disease, or personal data of the patients, should be kept within the cooperating organizations. However, in some cases, medical organizations, such as hospitals, do not approve of disclosing the medical records to anyone outside the organization, even to care managers or other hospitals.

Conflict of requirements between the aspect of information security and the network-centric operation often occurs in every situation where principles of network-centric operations should be implemented. While the aspect of infosec requires the confidentiality of delicate information,

adopting network-centric operations makes much of the system effective. Here we propose the solution satisfying the two conflicting requirements.



One of the typical examples of the information which is required both to protect and utilize is the individual medical record, such as the name of the disease (HIV, cancer, etc.) or some metabolic data (cholesterol, blood sugar, blood pressure, etc). Moreover, in many cases this information is linked with the personal information when it is utilized. This means that whenever the clinical information of a certain patient of HIV is used for a study, the information is associated with the age, sex, and location of the hospital. In other words, a utilization of the clinical information carries the risk of the leak of personal information. Otherwise no clinically effective study would be done. The contradiction of requirements is illustrated in the Figure 1. Development of medicine is achieved only by the clinical study based on the patients' data. Nonetheless, the patients' medical information contains, or is closely associated with, delicate personal information. Under the current technology, either of the two should be sacrificed, but it is only after solving the conflict that the real reassurance comes to the society.

2. Current situation of the Medicine and Care in Japan

Japan, which is facing the challenge of a hyper-aging society, needs advanced medical care closely related to the patients' life and nursing care. The desirable healthcare service includes home care, domiciliary care, terminal care, etc. Identifying the demand of the society, the government issued a plan in 2006 to reduce the number of hospital beds by the overhaul of the medical fee scheme, targeting the reduction of overall medical fees. The purpose of the plan is to correct the situation that the majority of the senior patients' cases are "social hospitalization" for non-medical reasons, where the patients are hospitalized although they can receive treatment at home. There are numerous cases in regional administration that the government conducts the policy of promoting home care, in which medical treatment and nursing care are closely aligned.

A similar tendency is observed in other countries. For example, Sweden, where as many as 14 percent of the nationals were above 65 years old already in 1980, has experienced that the elderly cannot leave hospitals to switch to ambulatory treatment, on account of the lack of the facilities. The hospitalization cost became a burden to the budget, and consequently the government decided to drastically reform the hospital care system in 1992. City administration officials offered facilities to accept the patients of "social hospitalization." The shift to the home care, or nursing care, resulted in the reduction of sickbeds by 28 percent in internal medicine, 48 percent in surgery, 74 percent in geriatrics, and 62 percent in psychiatry.

Cooperation based on shared awareness and synchronization among various organizations including hospital, nursing, care, care management, local government, pharmacy, and the suppliers of medical devices, is very important in improving the healthcare.

The medical and care services are also expected, as a growing industry, to lead the growth of Japanese economy. According to the Proposal issued by the Organization of Japanese Corporate Executives (December 14th of 2009), the healthcare industry is expected to employ 1.7 million people and have an impact of 12.7 billion US$ on the overall economy.

3. Expectation to the Medicine/Care Cooperation Network

One of the major tasks for the growth of healthcare services is to promote the effective utilization of patients' information, including historical records of medicine and care. Statistical analysis of numerous patients' data would generate the new knowledge necessary in creating new methodology of care services. It would result in the improvement of the quality of medical and care services. For that purpose, we have to overcome the issue of "protecting personal data" by actively utilizing the data.

When personal data is used in the development of medicine, delicate information of individuals is disclosed. The 'Protection of Personal Information' and the 'Utilization of Personal Information' are contradictory to each other, and therefore a solution to satisfy the both is desired. It is a difficult task, but once it is solved, the quality and effectiveness of the care service and healthcare would be extensively improved. And at the same time, the trust of the medical system would be established among citizens, based on the sense of security. These effects would lead to an effective healthcare network.

Figure 2 illustrates the healthcare network where metabolic and care data are contained. This system would structure an effective healthcare network by including the solution to solve the conflict shown in the Figure 1.

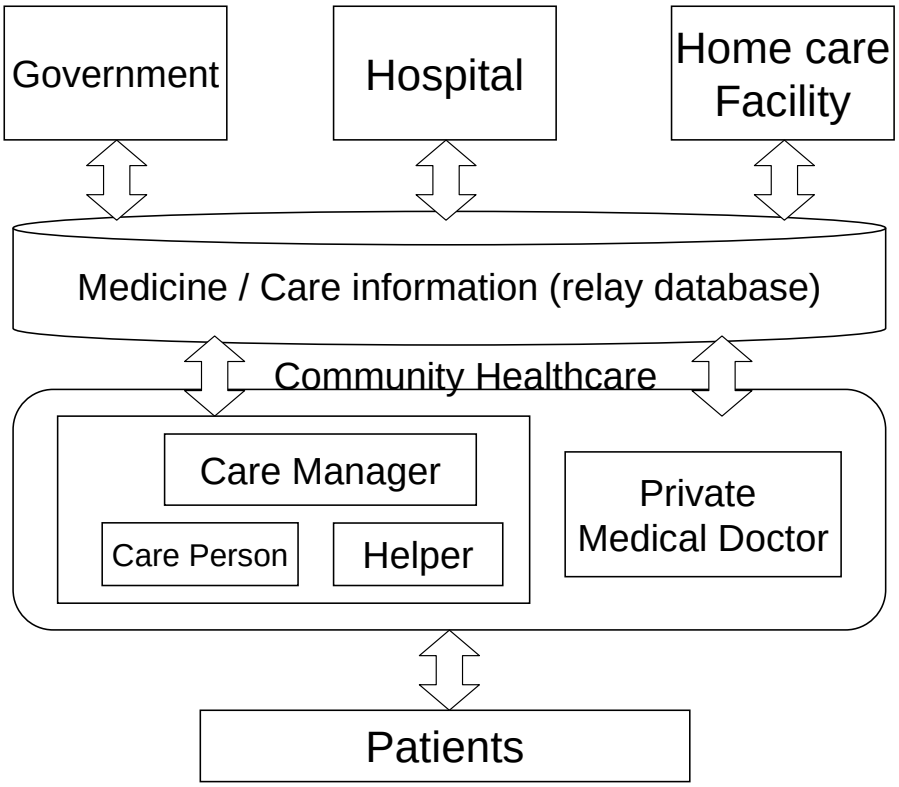


Figure 2: Medicine/Care Cooperation Network

4. Technical Features required to the Healthcare Network

The systems solving the “conflict of requirements” are listed below:

- A system to generate new knowledge from the individual medical information while protecting privacy, and thereby contribute to the progress of the medicine
- A system in which each user can post comments on the service and organization of the healthcare without disclosing private information
- A system in which “privacy” of the medical professionals are maintained. The security system to protect the information of the activity of acquiring knowledge and information
- A security system to prevent the people (such as the system managers of hospitals, or system managers of ASP) from malicious activity (such as falsification, unauthorized deletion, etc.)
- An audit system to verify that the data is properly processed.

5. The Proposed Approaches

We propose the following security systems for the Healthcare Network which we outlined above:

- A Data Processing system which enables the statistical processing of data while preserving

privacy

- An Anonymous Surveying system
- A Secure Information Search system
- A New Access Control system

The interaction between the medical and care network systems in the “Healthcare Network System” is shown in the Figure 3.

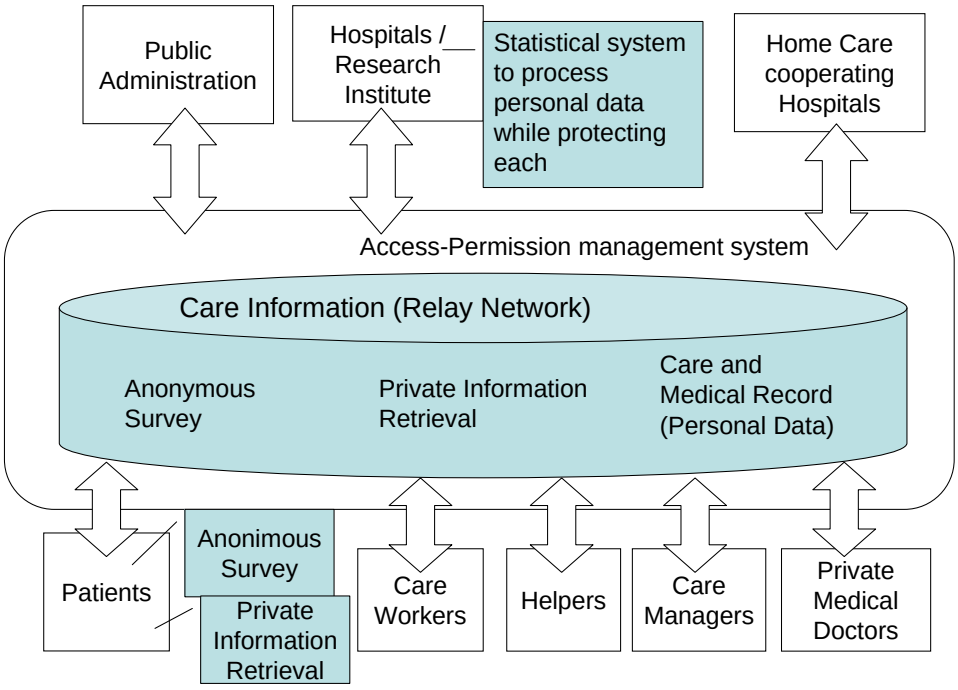


Figure 3: Interaction between Medical & Care network

(a) Privacy preserving information processing

If data mining is done to each piece of information about the medical care and the nursing care, new knowledge would be generated and the medical and care technology would be significantly improved. The methodology of “secure data mining” is emphasized these days. For example, a study of public health looking into the correlation between the DNA data and the pathogenesis of diseases is important. However, it would be difficult for individuals to disclose the information on biological vulnerability to diseases such as heart attack or diabetes. Usually, medical information should be associated with the personal data such as the personal identity or the information about the facilities where the data was acquired. Incidentally, in some cases the system managers might know the medical record of some individuals. Therefore, the validity of data should be assured while the individuals’ personal information is protected. Requirement of utilizing the medical data and protection of personal data are contradictory to each other. The conflict is difficult to

solve for existing IT security technologies such as cryptosystem and access control.

In order to solve the conflicting issues, we suggest the development of an interactive, cryptographic protocol using some cryptosystems as element technologies. The mechanism of privacy protection that ensures that“Users of the data can verify the data source, but the users cannot know the data themselves” has been focused on and continuously studied since Y. Lindel and B. Pinkes proposed the system of “Privacy Preserving Data Mining (PPDM).” An international conference on this theme, DIMACS/RORITA Workshop PPDM was held in 2004. Several systems to realize the processing of personal data while preserving the confidentiality have been proposed, including one utilizing secret function (secret sharing) or homomorphic public key cryptosystems, and Reconstruction-Based Techniques, which deliberately inject random numbers and restore the original data using the Bayes’ theorem.

It is necessary to process extensive personal information in Data Mining. Secret sharing protocol has emerged as a problem in performance and various studies have been made to overcome the problem. On the other hand, the “Duplicated Ciphering Protocol”[] of Tsujii et al., which has only two centers in the system, would be appropriate for the purpose. The practical safeguards considering the implementation of the secret key, and key management system are discussed.

Duplicated Ciphering Protocol:

Figure 4 illustrates the concept of “systems realizing the counting, statistics, and correlation.” Center 1 has the secret key of the public key cryptosystem (such as RSA) and publishes the public key. Center 2 has the secret key of the homomorphic cryptosystem and publishes the public key. Personal information is defined as the Personal ID and medical/care history. History data are encrypted with the public key of the Center 2 and subsequently with the public key of the Center 1 (duplicated encryption by two different systems). The duplicated ciphertext attached with the Personal ID is contained in the personal data. Center 1 checks the validity of the individual, and the ciphertext encrypted with the key of Center 2 is restored. Afterwards, the pieces of data are added together without decrypting them. And finally, Center 2 decrypts the product to acquire the sum.

Since Center 1 does not have the secret key of the Center 2, it cannot decrypt the ciphertext (it cannot know the medical history). On the other hand, Center 2 does not have the secret key of the Center 1. Therefore, it cannot associate the medical history with the Personal ID. The privacy is protected in this way.

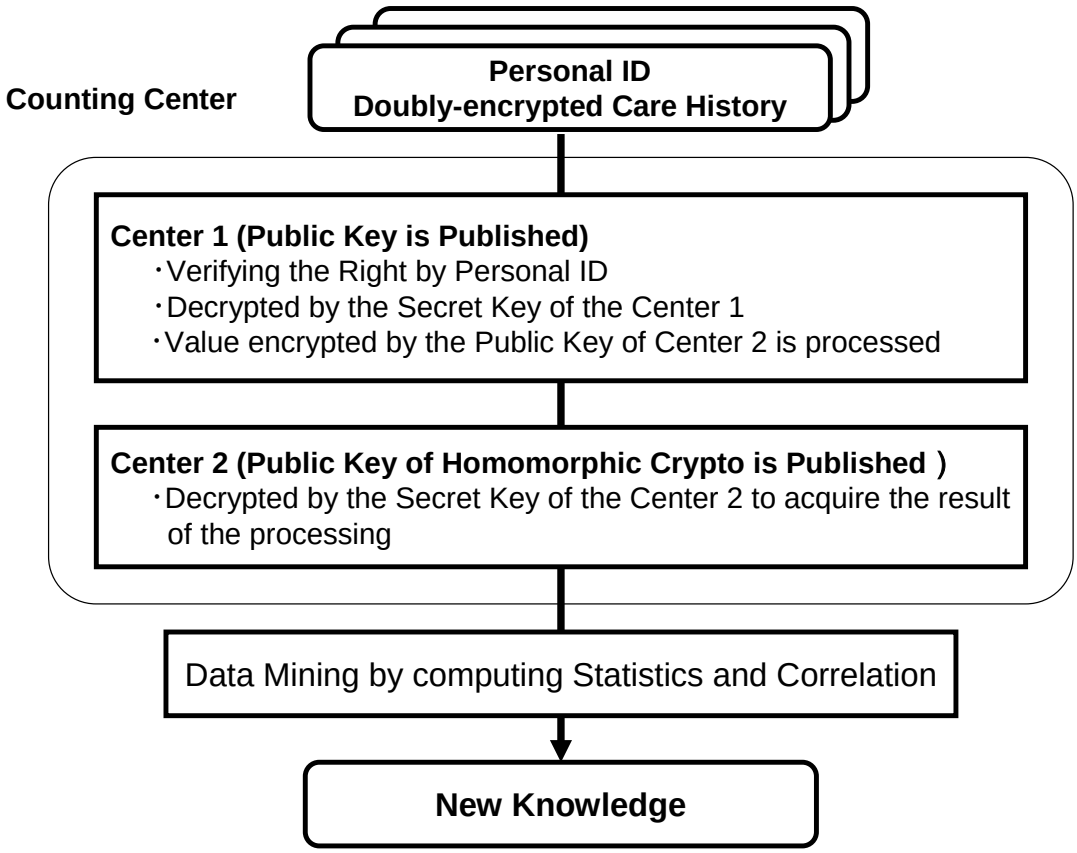


Figure 5: Data Processing system protecting the individual data

(b) Anonymous Opinion Survey system

Current practices of nursing care and healthcare require home nursing, where the operations of helpers are more difficult to manage than similar operations in dedicated facilities. Under this condition, abuse is expected. In order to manage the operation, evaluation by the customers is inevitable. It could be enabled by appropriately applying the technology of electronic voting.

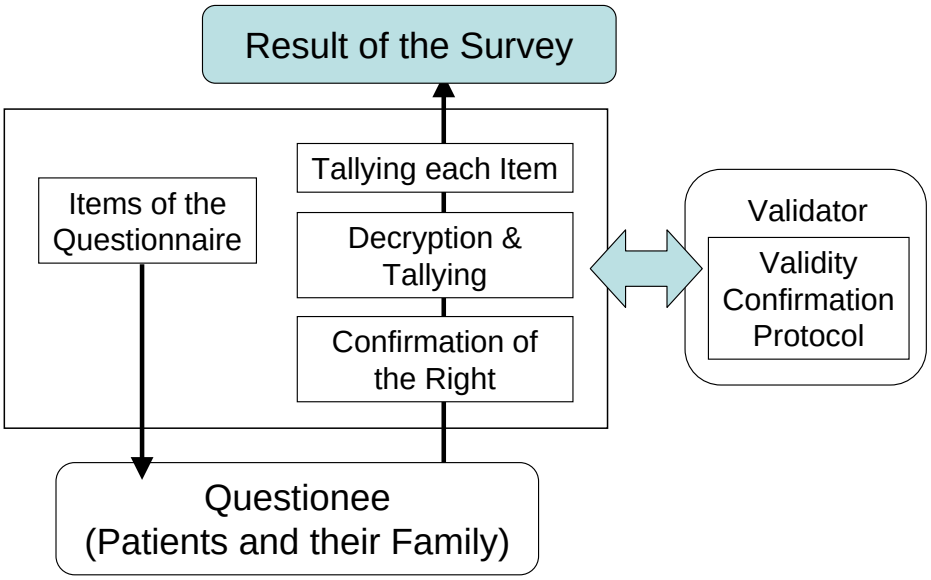


Figure 6: Anonymous Opinion Survey

(c) Private Information Retrieval

Situations where a search operation is used are increasing so rapidly that the necessity of protecting the personal information is pointed out. Especially, in the field of healthcare and nursing care, various kinds of search operations are needed in deciding the care plan. It is expected that considerable amount of information should be drawn from the history of search queries. This problem is identified also in the academic field as “Private Information Retrieval” (PIR), to protect the detailed information what is searched, while verifying the right of the operators to do the search. Like the protection of personal data, this is a solution which can satisfy contradicting requirements.

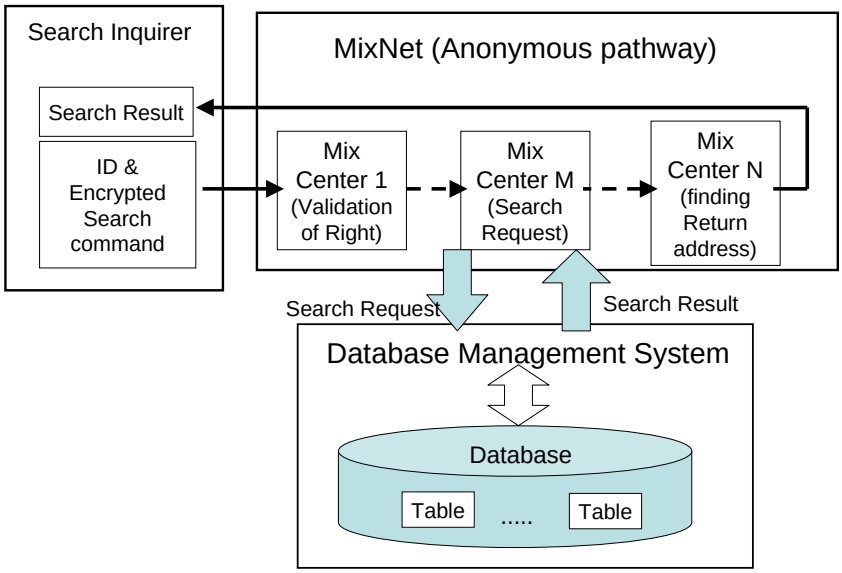


Figure 7: Secure Private Information Search System

(d) Information Access Control using the Next-Generation Cryptosystem

It is necessary to enable the setting of the access permission to personal medical/care history according to the role (physician, nurse, pharmacist, administration staff, etc) and organization structure. Although this kind of security systems is already developed, it is necessary to implement the system based on the newly developed cryptosystem for following reason:

- Sometimes it is possible for malicious system managers to obtain unauthorized access
- The operation of encrypting collective personal data is quite complicated in the existing cryptosystem, requiring the process of encrypting each data according to the faculty or condition.

We are planning a new system where access permission is defined according to the property of information suppliers and information users, as well as other condition. This design would improve the efficiency of the system, allowing the autonomous and distributed operation of defining access permission.

There are numerous kinds of information such as the name of the disease, body condition, history of disease of family, total medical bills, etc. Each of them has specific security requirements and access permission. This information would be appropriately protected by encrypting the whole and preparing secret decryption keys which allow partial decryption. This cryptosystem is a variant of the Stepwise Triangular System (STS), which Tsujii et al. proposed in 2010.

6. Conclusions and Future work

A security system for databases sharing information among different organizations is proposed. Regardless of the kind of operation and the nature of organizations, it is inevitable that information sharing itself becomes the security threat. The security problem results either in the abortion of the cooperation or in the reduced effect of the cooperation. For the successful implementation of “Power to the Edge,” it is necessary to develop a security system designed for each organization and operation.

7. Acknowledgements

The author owes a deep debt of gratitude to the members of Nagaokakyo chamber Ensemble including Kazunori Sato, Jyunko Hasegawa and Masters Orchestra in Japan Amateur Corp. who provided valuable insight. Professor Yukikazu Suzuki of Kurashiki Sakyo University has been enthusiastic about our ideas and has provided much helpful advice and comments. Hirohisa Wakao of the Federation of Japan Amateur Orchestra Corp. has inspired me through his constant activities on orchestra work.

This study is supported by the Project entitled “Developing the next-generation Information

Security Technology” of the Ministry of Economy, Trade and Industry (METI).

8. References

[1] D. von Lubitz, N. Wickramasinghe: “Healthcare and Technology: the doctrine of networkcentric healthcare,” International Journal of Electronic Healthcare, vol. 2, No. 4 (2006)

[2] H. Yamaguchi, “The design of a new service system based on the interdisciplinary research, IDPT, vol. 2, pp. 28-30 (2003)

[3] H. Yamaguchi, S. Tsujii, “Anonymous query language retrieval,” IEICE Technical Report vol. 109, No. 271, pp. 69-74 (2009)

[4] S. Tsujii, H. Yamaguchi, A. Kitazawa, K. Kurosawa: “A method for voting protocols with regards to privacy,” Technical report of IEICE, ISEC98, pp. 45-51 (1998)

Appendix (Terminology)

(1) Homomorphic Cryptosystem

Homomoriphism is a property that the ciphertexts corresponding to the plaintext m_1 and m_2 are multiplied, the product becomes the ciphertext of (m_1+m_2). When the encryption function E and the decryption function D are given, $D(E(m_1)\times E(m_2))=D(E(m_1+m_2))= m_1+m_2$

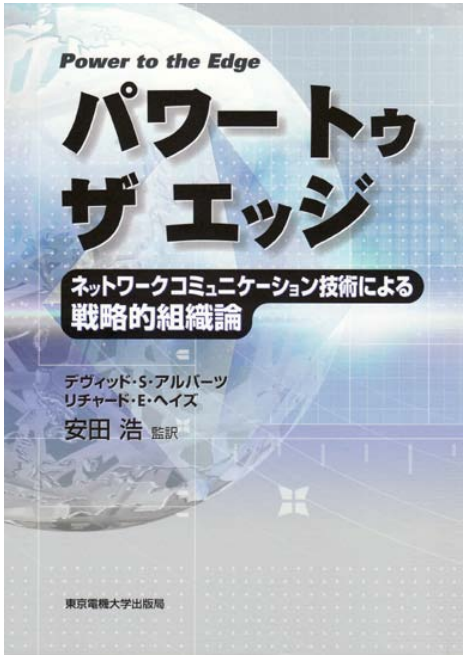
Privacy Preserving Service Discovery for Interoperability in "Power to the Edge" Approach

Research and Development Initiative,
Chuo University

Hiroshi Yamaguchi, Masahito Gotaishi,
Shigeo Tsujii, Norihisa Doi

“Power to the Edge” Approach for the non-Military Activity

- Masahito Gotaishi,
  - A member of the Japanese Translation team of “Power to the Edge”
  - Long for the application of “Power to the Edge” approach to Medicine and Care
- Hiroshi Yamaguchi
  - Once presented in ICCRTS (2009)
  - Application of PTE to control the performance of Orchestra
  - Best Paper of the Section



Problem to Solve

- Information is necessary in “Self-Synchronization” and “Shared Situation Awareness”
- Information is shared in the organization
- Typically information is shared with the partners
- These information are internal ones and often **Confidential**

Examples in the Real World

- e-Administration: Taxing, refund of high medical charge, allowance for female-headed household, etc.
  - Information is not widely shared within the public administration office
  - because it is “Personal Information”
- Medicine & Care: Making use of the chart data, result of the treatment, etc.
  - Strictly confidential
  - But medicine needs the data

Dilemma

- “Value” of the Information is realized ONLY WHEN it is used
- Usually solved by "Trade-Off."
- Is there a "Best of the Both World" solution ?

Our Proposal (medicine & care)

- Clinical data computed while they are encrypted (secret sharing) -assuming cloud computing
- Protecting the search operation information, while enabling semantic search
- Anonymous Feedback
- Access Control using Cryptosystem

Privacy Preserving Data Processing (PPDP)

Encrypted Medical Information DB (Personal Information)

Proof of validity Protocol

PPDP is correctly Processed (i.e. Personal Information Is not revealed)?

Privacy Preserving Data Processing

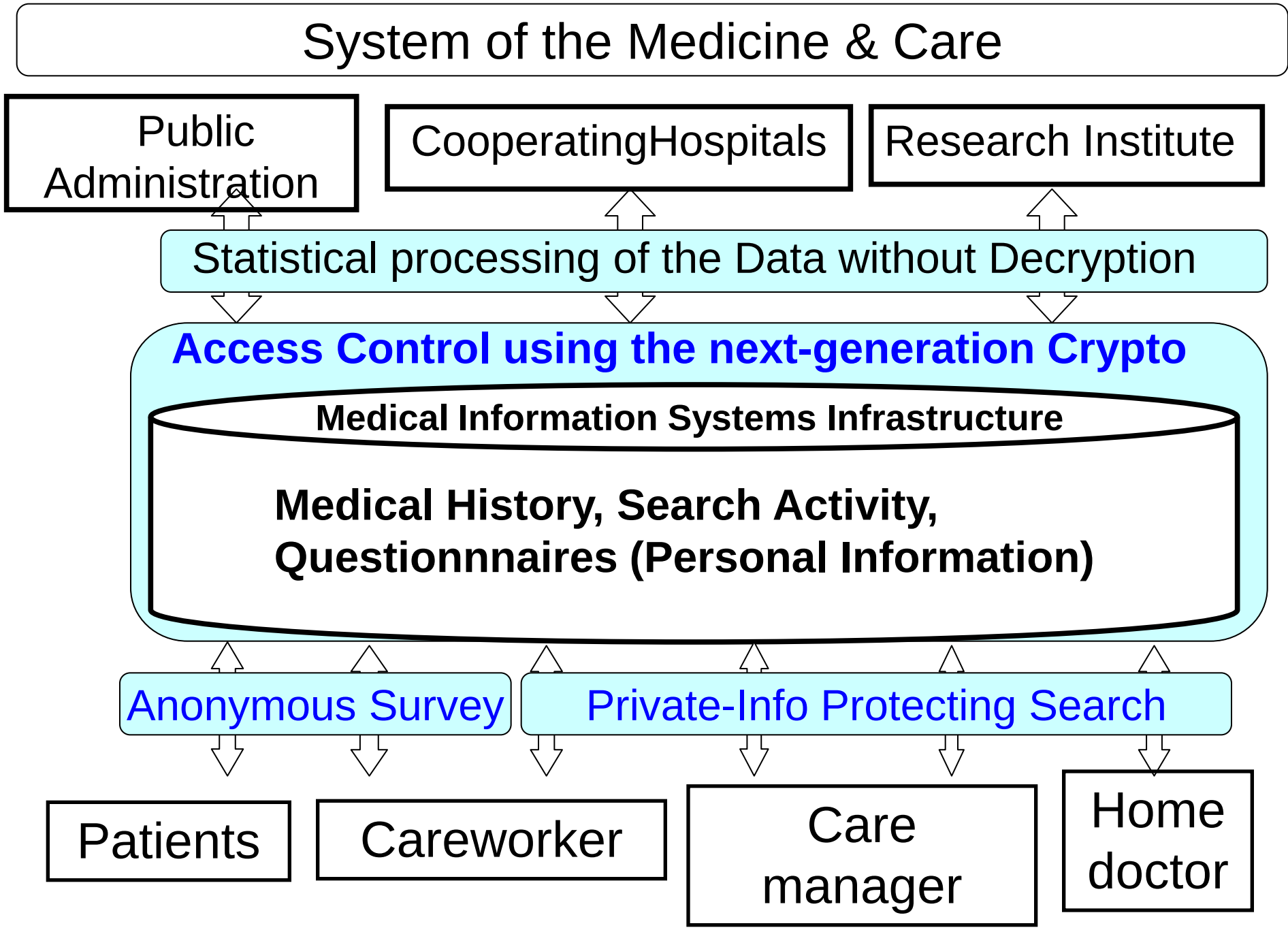
Functional Operation (∑,∏ etc.) ,while encrypted

Data Processing (Statistics, Mining etc.)

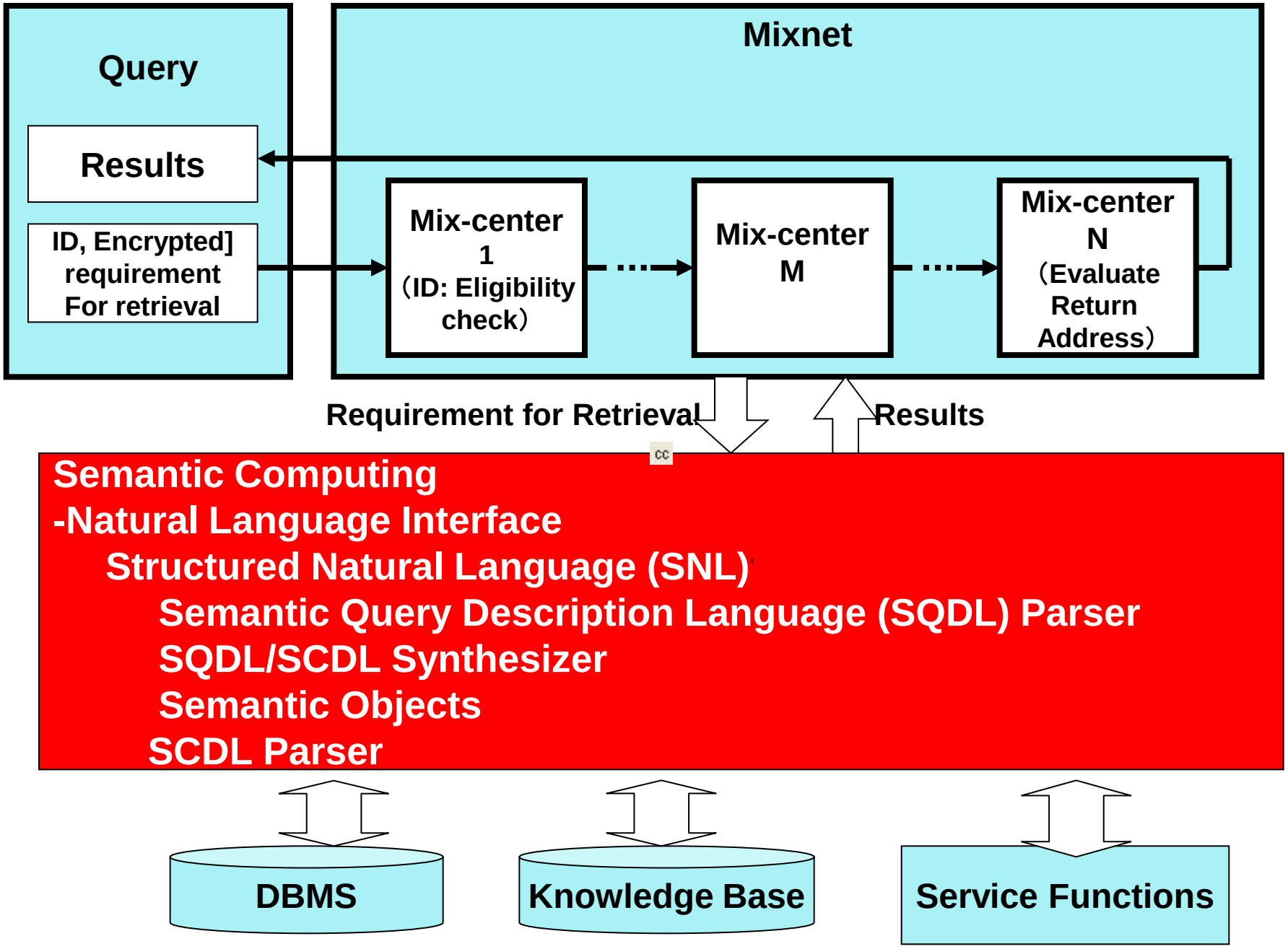
Semantic Computing (Natural Language, etc.)

Patients are able to confirm that their privacy are preserved. ‘Relieved!’

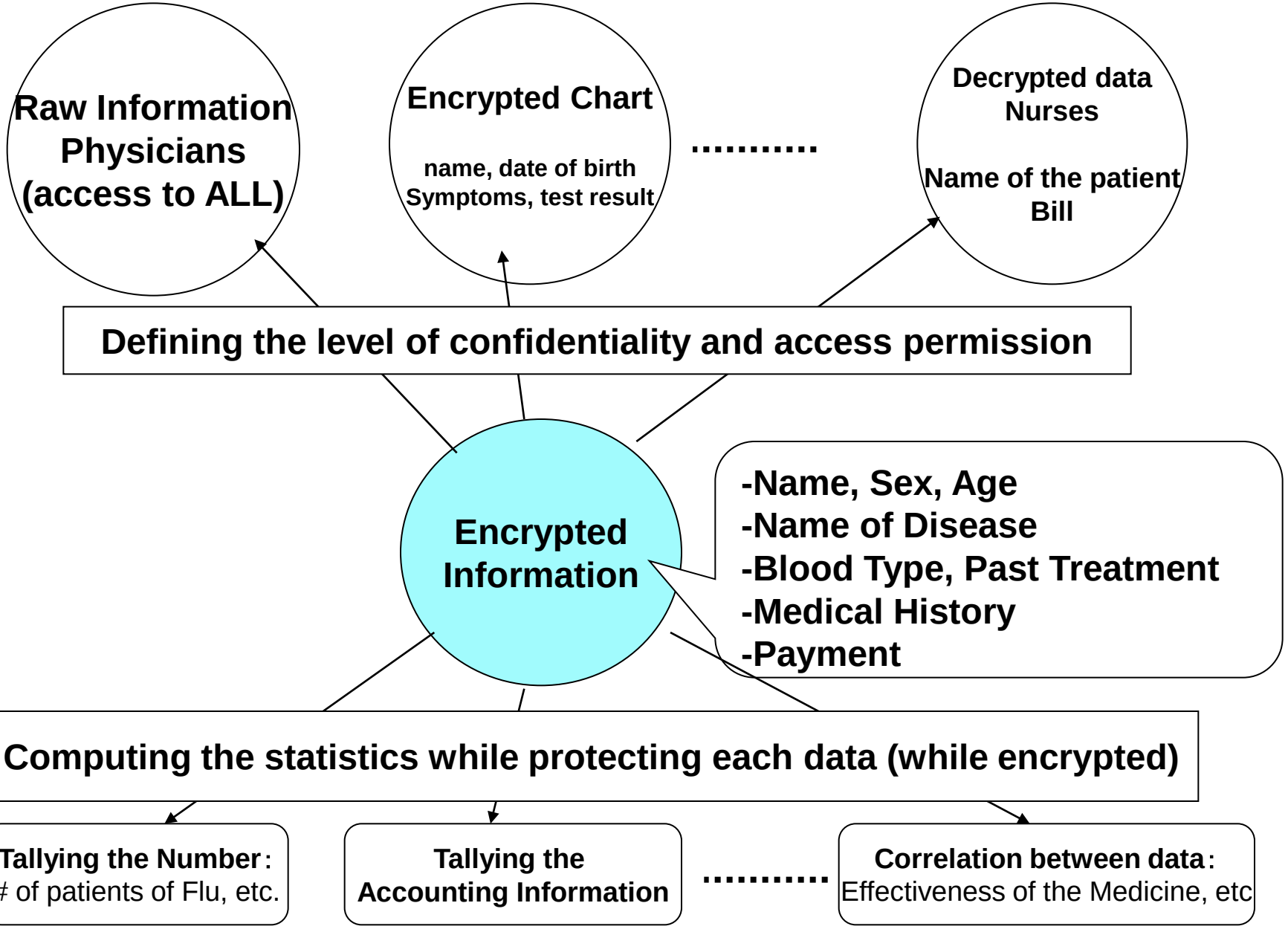
Medical researchers are able to obtain processed data without decrypting the encrypted data


System of the Medicine & Care
Public Administration
CooperatingHospitals
Research Institute
Statistical processing of the Data without Decryption
Access Control using the next-generation Crypto
Medical Information Systems Infrastructure
Medical History, Search Activity,
Questionnnaires (Personal Information)
Anonymous Survey
Private-Info Protecting Search
Patients
Careworker
Care manager
Home doctor

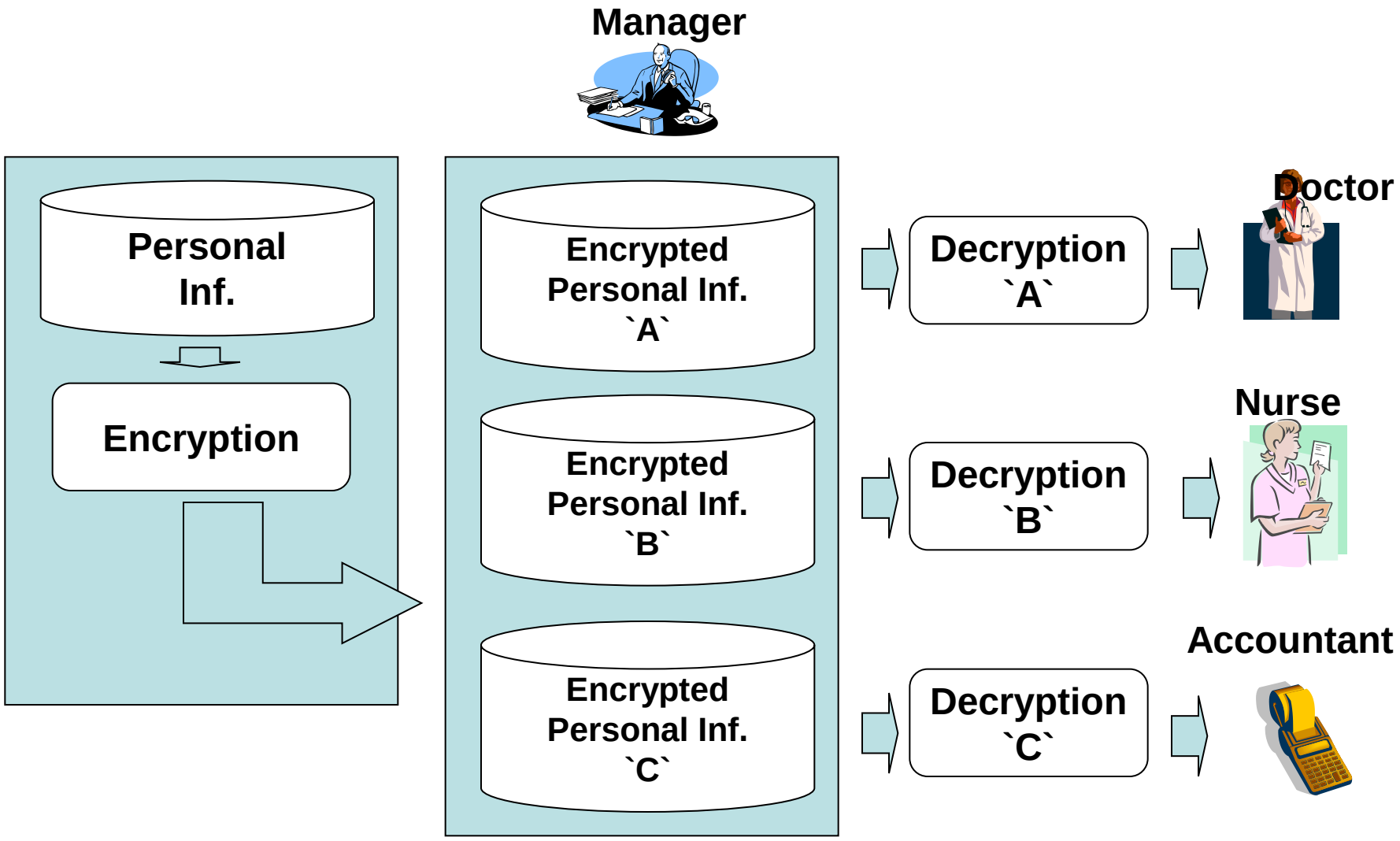
Private Information Retrieval including Content-based Multimedia Inf.



Access Control / Operation without Decryption

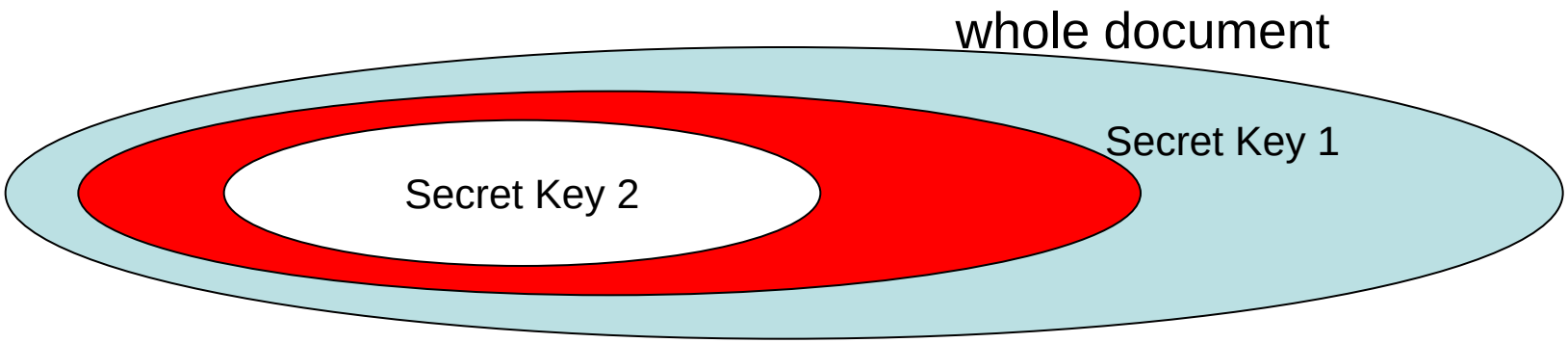


Access Control Scheme by Next Generation Cryptographic Algorithm



New Cryptosystem

- Multivariate Public Key Cryptosystem (MPKC)
- One of Post-Quantum Cryptosystems
- New feature, with an identical Public Key, the range of the decryption defers depending on Secret Keys



Difference between other Systems

	Our Cryptosystem	Conventional system
situation	Access control of the members of organization, depending on the responsibility	Usually designed for Access Control of individuals Control the access depending on the properties of individuals
usage	Dynamically Changes depending on the change of organization, new roles, etc..	Generally Static ,,,, whether the person is US national, over 21, bought the content,,,,
crypto-system	Multi-variate Public Key	ID-base, Pairing, elliptic-curve, ,,

Summary

- Confidential Information and detailed information of operation be protected
- Our proposal assumes medicine and care. But the system is applicable to any situation handling confidential information
- The system is fitted for the "Power to the Edge" organization

Thank you !

- Questions ?